Homeland Security

Daily Open Source Infrastructure Report for 8 December 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

For information, click here: http://www.dhs.gov

Top Stories

- KPMH 26 Visalia reports that a leak from a valve Monday led a rail tanker car in Fresno, California to spill 500 gallons of the toxic chemical magnesium bisulfite. (See item **5**)
- According to the Seattle Post-Intelligencer, federal charges have been brought against a Washington State man accused of attempting to send 300 satellite components to China. (See item **11**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *December 7, KATV 7 Little Rock* – (Arkansas) **Gas tanker explodes.** A gas tanker wrecked and bursts into flames injuring the driver and shutting down a south Pulaski County, Arkansas road. It happened around 8 p.m. December 6. Authorities said the driver of the truck exited Interstate 530, thinking he was taking the Sheridan Exit. Instead it was Bingham Road. That is when he drove off into a ravine and the truck erupted into flames. Bingham Road was shut down and authorities said it would be hours before it is reopened. "These types of fires, its best to be burned out," said a

Pulaski County Sheriff's Department spokesman. "Because of the quantity of fuel. So its contained right now and they are going to let it burn out and it will be one or two in the morning before it opens back up." No homes were in danger of the fire. The driver was taken to a local hospital.
Source: http://www.katv.com/Global/story.asp?S=13627796

2. *December 7, Associated Press* – (Maine) **Northern Maine gets walloped with snow.** Heavy snow fell across the northern half of Maine in the state's first major snowstorm of the season December 6, knocking out power for thousands of homes and businesses, closing scores of schools, and causing treacherous travel conditions. Nearly 1 foot of snow had fallen in many places by late afternoon, with 16 inches reported in the Penobscot County town of Lakeville. The National Weather Service was calling for some locations to get 20 inches by the time the snow stopped in the overnight hours. More than 2,000 homes and businesses were without power in the morning due to heavy snow, but the number of outages had fallen to a little over 800 by sunset, according to Bangor Hydro Electric Co. Route 9, the busy east-west highway from Calais to Bangor, was shut down for several hours after a number of tractor-trailer trucks slid off or blocked the road, but no injuries were reported. The storm caused businesses and courts to shut down for the day, while schools and universities, including the University of Maine in Orono, canceled classes.
Source:
http://www.bostonherald.com/news/national/northeast/view/20101207northern_maine_gets_walloped_with_snow/srvc=home&position=recent

3. *December 6, Associated Press* – (Washington) **Power restored in San Juan Islands.** Orcas Power and Light reports that an electrical outage cut off service to much of Washington State's San Juan Islands for more than 3 hours December 6. The outage began at 11:30 a.m. A utility spokesman said power was restored by about 3 p.m. The outage was caused by a problem at a Bonneville Power Administration substation. The outage affected about 9,000 customers on San Juan, Orcas, and Shaw islands.
Source:
http://seattletimes.nwsource.com/html/localnews/2013612080_apwasanjuansoutage2nd ld.html

4. *December 6, Lawrence Journal-World* – (Kansas) **Nearly 8,000 lose power as wide-ranging outage hits core of Lawrence; nearly all service restored within an hour.** Nearly 8,000 customers, about 18 percent of Westar Energy's customers in Douglas County, Kansas, lost power for about 1 hour December 6 after a wide-ranging power outage struck downtown Lawrence and numerous other areas. By 3 p.m., all of the more than 44,000 Douglas County customers had their power restored. The outage had affected an area that included parts of North Lawrence south to 15th Street and from at least New York Street west to Iowa Street. Most of the Kansas University campus had power throughout the outage. Dozens of traffic lights went out. A Westar Energy representative said the outage was caused by a faulty piece of underground equipment, and that crews estimated they were going to have power restored to all customers by 2:45 p.m.

Source: http://www2.ljworld.com/news/2010/dec/06/power-outages-strikes-downtown-surrounding-area/

[Return to top]

Chemical Industry Sector

5. *December 6, KMPH 26 Visalia* – (California) **Rail car spills hazardous material in southeast Fresno.** Shortly after 7:30 a.m. December 6, Fresno, California firefighters arrived on the scene of a hazardous material spill in southeast Fresno. A rail tanker car spilled close to 7,500 gallons of magnesium bisulfite onto the ground at Florence Avenue near Cedar. The battalion chief said the tanker began to leak from one of its bottom valves, but the cause is unknown magnesium bisulfite is used in agriculture as a fertilizer. Because the spill was isolated to the area, there appears to be no threat to the public. magnesium bisulfite is potentially dangerous through inhalation and is capable of burning skin. The toxic chemical was contained thanks to good weather conditions. The fire crews responding wore hazmat and respiratory gear to reduce contamination. The fire department said the U.S. Environmental Protection Agency and the owner of the container, Univar, are looking into clean-up options.
   Source: http://www.kmph.com/Global/story.asp?S=13624566

6. *December 6, WPTZ 5 Plattsburgh* – (Vermont) **Truck carrying potentially explosive chemical rolls over.** Emergency crews spent the afternoon of December 6 in Sheffield, Vermont where a truck carrying a potentially dangerous chemical slid off the road and into a stream. State police said the vehicle was traveling up New Duck Pond Road and lost traction. It then slid backwards and onto the shoulder of the road, tipping and rolling over towards the driver's side. New Duck Pond Road was closed for much of the day. The Maine Drilling and Blasting truck was carrying potentially explosive material. Police said there was never any danger to the public because the chemical only becomes explosive when it interacts with another chemical, which was not present. When the truck rolled over, police said the chemical itself did not spill, but haz-mat crews responded as a precaution. The department of motor vehicles will inspect the vehicle to try and determine why it was not able to drive up the hill.
   Source: http://www.wptz.com/r/26039737/detail.html

For another story, see item **21**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

7. *December 7, Nashville Tennessean* – (International) **TN could process foreign nuclear waste, then ship it back.** Italian or other foreign radioactive waste could be burned in Tennessee, but the company handling it said the ash and other remains will be sent back to the country of origin. A federal court ruling prohibits any of it from going to a Utah landfill. EnergySolutions, which wants to bring 20,000 tons of waste

from an old Italian nuclear plant to Oak Ridge, Tennessee, has asked the Nuclear Regulatory Commission to allow German radioactive refuse to be shipped to the United States. The company will take foreign waste only if the country from which it is shaped takes back the ashes or whatever remains after processing, the company spokesman said December 6.
Source:
http://www.tennessean.com/article/20101207/NEWS01/12070340/TN+could+process+foreign+nuclear+waste++then+ship+it+back

[Return to top]

Critical Manufacturing Sector

8. *December 6, Birmingham Business Journal* – (Alabama) **U.S. Pipe & Foundry workers strike.** Nearly 300 U.S. Pipe & Foundry steelworker union members in Bessemer, Alabama, began a strike December 5 over labor negotiations. The sub-district director of District 9 for the United Steelworkers said the strike began over unfair labor practices proposed by U.S. Pipe in its contract with steelworkers at its Bessemer operations, which expired December 4 after previous negotiations and two extensions. One of the main issues is U.S. Pipe is asking the steelworkers to combine jobs into one job class, with workers performing unsafe assignments with little or no training, the union claimed.
Source: http://www.bizjournals.com/birmingham/news/2010/12/06/us-pipe-foundry-workers-strike.html

9. *December 6, Car Advice* – (Ohio) **Keyless entry hacked by thieves.** According to reports, tech-enthused thieves are now able to hack into cars using codes given off by a car's keyless entry system. Reports have been circling in Ohio, whereby such capabilities have apparently been exercised. If such capabilities are possible, it would allow thieves to enter and exit a car without the owner knowing they have been robbed. The technology behind this has been circulated in an e-mail in the United States, warning colleagues and friends of what is possible. It basically explained that once a car is locked using the keyless entry device, a code is sent to the car. This code can then, apparently, be picked up by tech-minded thieves using a special tool. This tool then re-sends the code to the car, thus unlocking the doors.
Source: http://www.caradvice.com.au/94068/keyless-entry-hacked-by-thieves/

10. *December 3, Denver Examiner* – (International) **ATSB plan to prevent exploding Airbus A380 engines.** The Australian Transport Safety Bureau (ATSB) set forth a plan December 3 designed to prevent Rolls-Royce Trent 900 engines from repeating the near disaster encountered on Qantas Airways Flight QF32 November 4, when the No. 2 engine on a Qantas Airbus A380 exploded shortly after the aircraft took off from Singapore Changi Airport (SIN), causing massive damage to the airframe and control systems. The new directives spell out preventive maintenance inspections after only two flight cycles, using a fiber optic boroscope and video camera to inspect a critical engine structure, the bore hole of an oil feeder pipe, to look for asymmetrical wear, that

could cause a thinning in the pipe wall, eventual rupture, an oil leak, and lead to the turbine blades of the jet engine exploding and fragmenting into lethal missiles. Additionally, the ASTB, whose duties are similar to the National Transportation Safety Board (NTSB) in the United States, has recommended a software fix that will serve to detect runaway engine turbine speeds, and shut the engine down completely before a more critical incident could occur.
Source: http://www.examiner.com/airlines-airport-in-national/atsb-plan-to-prevent-exploding-airbus-a380-engines

[Return to top]

Defense Industrial Base Sector

11. *December 6, Seattle Post-Intelligencer* – (International) **Charge: Woodinville man tried to send military equipment to China.** Federal prosecutors have brought charges against a 46-year-old man from Woodinville, Washington, accused of smuggling military equipment to China. The suspect was arrested December 3 after nearly 2 years of investigation by the FBI. He is purported to have attempted to send 300 satellite components to China. He allegedly told an informant the parts were meant for the China Space Technology Co.'s spacecraft program. On another occasion, federal investigators contend the suspect said some of the parts would be used in the design of "China's new generation of passenger jet." Prosecutors contend he agreed to pay $620,000 to obtain the parts. The suspect is charged with conspiracy to violate federal arms control laws, which carries a maximum term of 5 years in prison.
Source: http://blog.seattlepi.com/seattle911/archives/230765.asp

[Return to top]

Banking and Finance Sector

12. *December 7, Softpedia* – (International) **Fake Google and Facebook joint prize campaign leads to Zbot.** Security researchers warn spam e-mails suggesting a joint prizes giveaway campaign from Google and Facebook eventually lead to a variant of the Zbot banking Trojan. The fake e-mails purport to come from "Google and Facebook team." The message suggests Google and Facebook, have decided to join together to give prizes away to users. The e-mails read: "Dear subscriber, As you may know, the holidays are just around the corner, so all of us here at Google and Facebook decided to come together and bring you a new contest with lots of prizes, including, but not limited to, the new Google Chrome OS which will be released in January 2011, Nexus One smartphones, Google Maps GPS for your favourite mobile phone and lots more. Think of it as our way of saying: 'Thank you!' for supporting our work all this time. For a chance to win, all you have to do is go to the attached page and follow the instructions. Hope you enjoy, Google & Facebook." Two of the three mentioned prizes are actually free products, and all are from Google. The attached file is called "Google & Facebook.html" and contains obfuscated JavaScript code. When opened inside a browser it redirects to a Web site that serves an exe file. According to BitDefender

security researchers, the file is a trojan downloader written in .NET that requires the .NET Framework installed on the targeted system in order to run. The original dropper installs a secondary downloader that distributes several information stealing Trojans, including Zbot.
Source: http://news.softpedia.com/news/Fake-Google-and-Facebook-Joint-Prize-Emails-Lead-to-Zbot-170972.shtml

13. *December 7, Associated Press* – (Oregon) **FBI: 2 arrests 20 minutes after Ore. bank robbery.** The FBI said it took just about 20 minutes for authorities to arrest two women after a robbery at a Clackamas, Oregon, credit union southeast of Portland. An FBI spokeswoman said witnesses report that a woman walked into a Rivermark Community Credit Union about 5 p.m. December 6 and demanded cash. The spokeswoman said the robber left with an undisclosed amount. At about 5:20 p.m., investigators surrounded a southeast Portland home and arrested the two female suspects. The two were booked into the Multnomah County Jail for investigation of bank robbery. The Oregonian said the Clackamas County sheriff's office, Portland police, and the FBI were involved in the investigation.
Source: http://www.statesmanjournal.com/article/20101207/UPDATE/101207005/-1/update

14. *December 6, Softpedia* – (International) **ZeuS-related fake electronic tax payment emails are back.** Security researchers warn of a new wave of fake Electronic Federal Tax Payment System (EFTPS) e-mails directing users to drive-by download Web sites that distribute the ZeuS banking Trojan. The fake e-mails claim the recipient's electronic tax payment was rejected due to a error in the submission form. They read: "Your Federal Tax Payment ID: ######## has been rejected. [where # is a digit] Return Reason Code R21 - The identification number used in the Company Identification Field is not valid. Please, check the information and refer to Code R21 to get details about your company payment in transaction contacts section: http://eftps.gov/R21 In other way forward information to your accountant adviser. EFTPS: The Electronic Federal Payment System PLEASE NOTE: Your tax payment is due regardless of EFTPS online availability. In case of an emergency, you can always make your tax payment by calling the EFTPS." It seems the attack targets businesses that would be forced to use EFTPS as default tax payment method starting from January 2011. According to security researchers from M86 Security, who analyzed the e-mails, the included link takes users to an attack page that tries to exploit vulnerabilities in outdated versions of Java and Adobe Reader. In particular, the exploit pack targets four vulnerabilities in Java and one in Adobe Reader. Successful exploitation of any of them results in a variant of the ZeuS banking Trojan being installed on the system.
Source: http://news.softpedia.com/news/ZeuS-Related-Fake-Electronic-Tax-Payment-Emails-Are-Back-170853.shtml

15. *December 6, Los Angeles Times* – (California) **West Covina man sentenced to prison for Ponzi scheme.** A West Covina, California man was sentenced December 6 to 11 years and 3 months in federal prison for running a Ponzi scheme that brought in about

$4 million from more than 107 victims. The convict was also ordered to pay $2,200,771 in restitution to his victims, whom he lured into his investment scheme by promising "guaranteed" annual interest rates as high as 120 percent, according to the U.S. attorney's office in Los Angeles. The convict, who is a Mexican national, was sentenced by a U.S. District Judge. He was arrested in October 2009 after the FBI searched his West Covina business, New Golden Investments Group, also known as NGI Group, the U.S. attorney's office said. The convict was indicted in May, and on September 17 he pleaded guilty to one count of mail fraud, one count of money laundering, and one count of misuse of a Social Security number, the statement said.
Source: http://latimesblogs.latimes.com/money_co/2010/12/west-covina-ngi-group-ponzi-scheme.html

[Return to top]

Transportation Sector

16. *December 6, Associated Press* – (National) **Dog bites 2 on airplane.** A US Airways flight headed to Phoenix, Arizona, made an emergency landing in Pittsburgh, Pennsylvania, after a dog on board bit a passenger and a flight attendant. A US Airways spokesman said the flight left Newark, New Jersey, December 6. He said a passenger carrying a dog let the animal out of its carrier and it bit the two people. The severity of the bites was not known. The pilot decided to land in Pittsburgh to make sure everyone was all right. US Airways allows passengers to carry certain pets if they are secured in approved carriers and kept under their seats, the spokesman said.
Source: http://voices.washingtonpost.com/dr-gridlock/2010/12/dog_bites_2_on_airplane.html

17. *December 6, Springfield News-Leader* – (Missouri) **Ozark man pleads guilty to making, selling fake aircraft inspection labels.** A 58-year-old man from Ozark, Missouri, has pleaded guilty in federal court to making and selling fake aircraft inspection labels. He is the owner of Air & Marine Radio, LLC, in Ozark. From March to September 2009, he created fraudulent Federal Aviation Administration inspection labels on his computer. The man also sold the false labels to multiple parties for $100 per label on multiple occasions, knowing that the labels would be placed in aircraft maintenance logbooks in violation of federal law.
Source: http://www.news-leader.com/article/20101206/BREAKING01/101206015/1007/NEWS01/Ozark+man+pleads+guilty+to+making++selling+fake+aircraft+inspection+labels

18. *December 6, Baltimore Sun* – (Maryland) **Fire closes Metro station, diverts bus routes.** A five-alarm fire in the 400 block of East Baltimore Street in Baltimore, Maryland December 6 forced the evacuation of the Shot Tower Metro Station and the diversion of seven Maryland Transit Administration (MTA) bus routes. An MTA spokesman said transit agency police shut the Shot Tower station because of a buildup of smoke from the fire. He said there were no injuries, but trains were running directly from Charles Center to Johns Hopkins Hospital without stopping at the station. Seven

bus routes that normally run on Baltimore Street were diverted onto Pratt Street. The Downtown Partnership reported that westbound traffic was diverted down South Street to Lombard Street. Eastbound traffic was diverted to Pratt Street, and from Pratt Street to President Street.
Source:
http://weblogs.baltimoresun.com/news/traffic/2010/12/fire_closes_metro_station_dive.html

19. *December 5, WHAM 13 Rochester* – (New York) **Bridge closure's impact.** There was no immediate danger according to New York's State Department of Transportation (DOT), however, DOT December 3 saw enough safety problems to close the Canandaigua Road Bridge in Macedon. DOT said calls were made to numerous officials, but because of the threat to public safety, engineers decided the bridge had to be closed immediately. Signs are posted on both sides of the bridge explaining it is closed. There were no clear detour routes in place as of December 4. The Canandaigua Road Bridge handled about 5,000 vehicles per day, DOT said. There are plans to rebuild or replace the bridge, but the earliest that process could begin would be 2013, DOT noted.
Source: http://www.13wham.com/news/local/story/Bridge-Closures-Impact/d3Qr6TKHgkSKe0duotGvmQ.cspx

20. *December 3, WRC 4 Washington D.C.* – (Maryland; District of Columbia) **Slick Beltway roads caused by chemical error.** The Maryland State Highway Administration (MSHA) said it is taking responsibility for slick roads December 3 that led to at least eight accidents on the Outer Loop of the Beltway. The accidents were reported December 3 near the Georgia Avenue and Connecticut Avenue exits. They caused significant backups, and four people were transported to local hospitals with minor injuries. MSHA said a section of the Outer Loop between Route 650 and Interstate 270 was pre-treated with what they thought was salt brine, which is what is usually used on area roads. However, MSHA said one of their trucks was using a mixture of salt brine and liquid magnesium. MSHA said that mixture is used only when there is actually snow on the ground. In this case, the mixture caused slick road surfaces. MSHA said the wrong mixture was used because the truck had not been reset from last winter. The truck might also be responsible for several accidents along Route 29, where the truck turned around to get on the Beltway.
Source: http://www.nbcwashington.com/news/local-beat/Officials-Investigate-Possible-Slick-Beltway-Roads-111254489.html

21. *December 2, Progressive Railroading* – (National) **Railroad Research Foundation obtains USDOT grant for TIH routing tool.** The U.S. Department of Transportation recently awarded Association of American Railroads affiliate Railroad Research Foundation (RRF) a $1.5 million Railroad Safety Technology Grant to implement a risk management tool for railroads to comply with federal regulations governing hazardous materials transportation. RRF will use the proceeds to enhance and implement the Rail Corridor Risk Management System, a Web-based software tool designed to analyze the safest, most secure routes to transport certain hazardous

materials. The technology is being developed in partnership with the Federal Railroad Administration, Federal Emergency Management Agency, Transportation Security Administration, and the Pipeline and Hazardous Materials Safety Administration. Federal regulations require railroads to conduct ongoing, comprehensive risk analyses of primary routes used to ship certain hazardous materials, as well as alternative routes. The analyses include at least 27 specific risk factors, as well as input provided by state and local governments.
Source: http://www.progressiverailroading.com/news/article/Railroad-Research-Foundation-obtains-USDOT-grant-for-TIH-routing-tool--25174

For more stories, see items **2**, **5**, **6**, and **50**

[Return to top]

Postal and Shipping Sector

22. *December 7, WFOR 4 Miami* – (National) **25K reward offered in mail carrier's murder.** A $25,000 reward is being offered by the U.S. Postal Service to anyone who can help lead police to the person who shot and killed a mail carrier in Miami, Florida, December 6 and then took off in his postal truck. The 60-year-old victim was gunned down just before 3 p.m. in the 400 block of Northwest 165 Street in North Miami-Dade County. Just a few blocks from the shooting, police found the victim's delivery truck abandoned. The killer ran away and eluded dozens of federal agents and police officers. A Miami-Dade Police official said the suspect was wearing a red jacket with a black t-shirt underneath. The suspect also has long dreads in his hair. Police do not have a motive for the deadly shooting.
Source: http://cbs4.com/local/miami.dade.police.2.2037354.html

23. *December 7, KSAZ 10 Phoenix* – (National) **Postal service fights counterfeit stamps.** As the U.S. Postal Service (USPS) grapples with service cuts and massive budget shortfalls, an estimated $134.4 million of its annual revenue is quietly slipping away to counterfeiters and perpetrators of other types of postal fraud, FOXNews.com reported December 6. Counterfeit stamps have been identified as a steady, recurring risk for USPS, which reported a loss of $8.5 billion in the last fiscal year — and they are one of the 10 biggest threats to USPS revenue, according to the 2009 annual report of the U.S. Postal Inspection Service, the law enforcement arm of USPS. Bogus stamps affect the consumers who buy them, too. People who buy stamps online or at local stores are at risk of unknowingly purchasing counterfeits — and then having their mail returned unopened.
Source: http://www.myfoxphoenix.com/dpps/news/postal-service-fights-counterfeit-stamps-dpgonc-20101207-fc_10974243

24. *December 7, Bloomberg* – (National) **UPS expands photo ID requirement for retail shipping.** United Parcel Service Inc. (UPS) will require customers shipping packages to show government-issued photo identification in an effort to intensify security after explosives were found on October cargo flights. The new policy expands a previous

rule in place at UPS Customer Centers to include all retail outlets. Customers without a pre-printed shipping label will have to display an ID, Atlanta-based UPS said in a statement December 7. "Since retail centers experience a significant increase in business from occasional shippers during the busy holidays, this enhancement adds a prudent step in our multilayered approach to security," the vice president of small business and retail marketing said in the statement.
Source: http://www.bloomberg.com/news/2010-12-07/ups-expands-photo-id-rule-for-retail-shipping-as-bombs-spur-security-steps.html

[Return to top]

Agriculture and Food Sector

25. *December 7, KTUL 8 Tulsa* – (Oklahoma) **Truck hauling chicken manure overturns, ramp reopen.** Crews are trying to figure out how to clean up a major mess December 7 at Interstate 44 and the Broken Arrow Expressway in Tulsa, klahoma. A semi hauling chicken manure overturned as it came around the ramp from westbound BA Expressway to I-44 westbound. Workers are trying to clean up the spilled manure. Tulsa Fire Department's hazardous materials team is also on hand to help.
Source: http://www.ktul.com/Global/story.asp?S=13628568

26. *December 7, Fast Company* – (Pennsylvania) **Convenience stores get action-packed with emergency preparedness schemes.** Food supplies have the potential to get massively cut during emergencies and that is why the Pennsylvania Department of Agriculture (PDA) is enlisting the help of the Pennsylvania Convenience Store Council (PCSC) to help draft protocols on how to manage food shortages in times of emergency. The private sector and public sectors are forging new partnerships in the state of Pennsylvania — especially as winter sets in and the incidence of major storms, power outages, and road closures skyrocket. Together with the Pennsylvania Food Merchants Association, the PCSC represents more than 1,100 retail food and convenience stores, wholesale distributors and other associated business members throughout Pennsylvania. The use of real-time, two-way sharing of situational awareness information will play a crucial role in the partnership with PDA.
Source: http://www.fastcompany.com/1707871/convenient-stores-go-action-packed-in-new-emergency-preparedness-schemes

For another story, see item **5**

[Return to top]

Water Sector

27. *December 4, New Canaan Patch* – (Connecticut) **Computer glitch shuts down water plant.** An early morning computer failure December 4 at the First Taxing District's Water Department filtration plant on Valley Road in New Canaan, Connecticut, caused water to flow across the roadway. The plant resumed operating before 8 a.m., the

district general manager said. He said residents along Valley Road may find their water discolored, and suggested they let the water run until it clears. The water is safe to drink, he said. A computer shut down in the plant, causing it to stop processing water. However, water continued to be pumped into the building from the adjacent reservoir, eventually causing water to rise up from a manhole and across Valley Road.
Source: http://newcanaan.patch.com/articles/computer-glitch-shuts-down-water-plant

28. *December 3, U.S. Environmental Protection Agency* – (Kansas) **Order issued to Kansas Department of Transportation to correct construction stormwater issues along U.S. Highway 59 project.** Environmental Protection Agency (EPA) Region 7 has issued an administrative compliance order to the Kansas Department of Transportation (KDOT), directing it to correct a series of violations of a stormwater permit issued for the U.S. Highway 59 construction site in Douglas and Franklin counties of Kansas. EPA inspectors visited the site in August 2010 to evaluate KDOT's management of stormwater and determine whether it was in compliance with permit requirements. EPA's inspection found numerous areas where sediment control was inadequate or altogether lacking. Several areas lacked silt fencing, berms or other equivalent means of controlling sediment moved by stormwater runoff. Along the project, stormwater, snow melt, drainage and runoff carries sediment and contaminants into unnamed tributaries of the West Fork of Tauy Creek and the Wakarusa River. EPA's order notes a series of violations, including failures to install and properly maintain adequate best management practices to control stormwater; failures to develop, properly implement, update and amend a stormwater pollution prevention plan; and failures to adequately document site inspections and comply with site inspection requirements. The order requires KDOT to submit a report to EPA within 30 days, detailing specific actions it has taken to correct the violations.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/e77fdd4f5afd88a3852576b3005a604f/dc2e2d473b057d83852577ee00609e50!OpenDocument

29. *December 2, U.S. Environmental Protection Agency* – (Massachusetts) **Billerica, Mass. manufacturer to pay fine to settle Clean Water Violations.** A company in Billerica, Massachusetts, that makes X-ray detection and related equipment has agreed to pay $40,000 to settle U.S. Environmental Protection Agency (EPA) claims it violated the Clean Water Act (CWA). According to EPA's New England office, American Science & Engineering (AS&E) discharged without authorization stormwater associated with industrial activity. The stormwater was discharged into wetlands adjacent to a Shawsheen River tributary. AS&E disclosed its violations to EPA and took some measures to minimize storm water runoff, but the company did not meet all legal requirements, nor all the requirements of EPA's self-disclosure policy. EPA took the company's disclosure into consideration in setting the penalty.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/e77fdd4f5afd88a3852576b3005a604f/aa76baf801006a54852577ed00564d78!OpenDocument

[Return to top]

Public Health and Healthcare Sector

30. *December 7, WebMD Health News* – (Georgia; National) **Georgia tops U.S. in seasonal flu activity.** So far, Georgia is the state hit the hardest by this year's influenza virus, according to the Center for Disease Control and Prevention (CDC). "Georgia is reporting high levels of influenza-like activity," the director of the CDC's National Center for Immunization and Respiratory Diseases said at a December 6 news conference. "It gets a 10 of 10, and is leading the country in terms of what we will be seeing." The flu — largely influenza type B — has been reported throughout Georgia, and been seen mainly in school-aged children, she said. Officials said this year's flu vaccine, which is recommended for everyone older than 6 months, is likely a good match for this year's flu, she said. "Some H1N1, an A/H3N2 strain, and B-strains have been seen this year, [along with] a mixture of B strains and A strains that haven't been characterized," she said. This year's vaccine protects against seasonal flu and the H1N1 swine flu. About 160 million doses of the vaccine have already been distributed nationwide, she said.
Source: http://www.webmd.com/cold-and-flu/news/20101206/georgia-tops-us-in-seasonal-flu-activity

31. *December 7, Associated Press* – (Florida) **Another confirmed case of cholera in Florida.** Miami, Florida health officials said test results confirmed that an American Airlines passenger who became ill on a flight from the Dominican Republic to Miami November 25 had cholera. The Miami-Dade Health Department released the results December 6. Officials said the man was a doctor who had been treating cholera patients. This marks the third confirmed case in Florida. State health officials said a Collier County woman and an Orlando-area women have recovered from cholera linked to an outbreak in Haiti.
Source: http://www.cbs12.com/news/cholera-4729943-case-haiti.html

32. *December 6, Allentown Morning Call* – (Pennsylvania) **LVHN fires doctor after patient records shared.** Lehigh Valley Health Network (LVHN) of Pennsylvania has fired an internist after determining he delivered personal information, including names, genders, addresses, ages, dates of birth, telephone numbers, and types of health insurance, on thousands of patients to another network to which he was applying. LVHN released the doctor after he gave out the information on more than 2,200 patients to a "concierge" medical network called MDVIP, an LVHN spokesman said. The network December 3 sent letters to the doctor's patients explaining why he was dismissed, the spokesman said. LVHN asserts releasing patient information could be a violation of the federal Health Insurance Portability and Accountability Act (HIPAA). MDVIP denies it violated HIPAA. In a statement, LVHN said it was ending its relationship with the doctor through Lehigh Valley Physician Group, an affiliate of the network, following "the unauthorized disclosure of demographic information about many LVPG patients being treated by him." The spokesman said medical records were not included in the release. The information was provided to MDVIP, a physician network based in Florida, in April, and LVHN learned of it this summer. LVHN then began an investigation, and the doctor eventually admitted to providing demographic

records to MDVIP.
Source: http://www.mcall.com/health/mc-allentown-lvh-kender-20101206,0,777284.story

33. *December 6, Associated Press* – (International) **Gunmen kill 4 in attack on 2 Mexico rehab centers.** Mexican police said armed commandos attacked two drug rehabilitation centers in Ciudad Juarez, Mexico, across from El Paso, Texas, killing four people and wounding five. A municipal police spokesman said the attacks occurred December 5. Three were killed in one center and one was killed in another. Gangs have killed dozens in drug rehabilitation centers in the last 2 years across Mexico, including nine last summer in Durango in the north, and 19 in Chihuahua city, capital of the border state where Ciudad Juarez is located. Cartels run the centers in some cases to recruit addicts, leaving them open to attacks from rivals.
Source: http://www.google.com/hostednews/ap/article/ALeqM5jFbXWwg2kUiswnDVBF7E1fLj2vrg?docId=9c9c7dd5bdee4212b9293b3e5d74752f

[Return to top]

Government Facilities Sector

34. *December 7, Associated Press* – (International) **Georgia arrests 6, calling them agents for Russia and accusing them of staging blasts.** The Republic of Georgia arrested six people suspected of being agents for Russia and accused them of staging a series of explosions, including one outside the U.S. Embassy in the capital, officials said December 7. The deputy interior minister said the suspects were recruited by the Russian military. A series of spy flaps has aggravated tense relations between the two former Soviet republics. The deputy said the six people, four men and two women, are accused of staging an explosion outside the U.S. Embassy in September, that caused no injuries, and several other blasts, including a blast in November outside the Labor Party's offices in Tbilisi that killed a woman. The deputy said that the suspects, all of them Georgian citizens, were arrested over the weekend. She said authorities had confiscated explosives and weapons during searches at their homes. The deputy said that two other suspected members of the group were hiding in Georgia's Russia-backed breakaway province of Abkhazia.
Source: http://www.brandonsun.com/world/breaking-news/georgia-arrests-6-suspected-russian-agents-accused-of-staging-explosions-outside-buildings-111433254.html?thx=y

35. *December 7, Albany Herald* – (Georgia) **Explosive found near MCLB.** Officials with Marine Corps Logistics Base (MCLB) in Albany, Georgia, have confirmed that explosive materials were found inside a tactical vehicle near the installation's truck gate December 3. An MCLB Albany spokesman said that an investigation has been launched to determine both how the explosives found their way to the location and exactly what the explosives were. In a statement, a spokesman said that around 5:35 p.m. December 3, base officials discovered the explosives inside what they called a "tactical vehicle," located near the MCLB's truck gate. The area was secured and the

material has been taken to an "isolated and safe area." Small scale evacuations of the immediate area were ordered and no one was injured, officials said.
Source:
http://www.albanyherald.com/news/headlines/Explosive_found_near_MCLB_111403104.html?ref=104

36. *December 7, South Florida Sun Sentinel* – (Florida) **Woman suspected in threats leading to schools lockdown has Fort Lauderdale hearing.** The woman arrested in connection with shooting threats that prompted a code red lockdown of the nation's sixth-largest school district is back in South Florida and is scheduled to have a federal magistrate's hearing in Fort Lauderdale December 7, authorities said. The suspect arrived in South Florida about 6 p.m. December 6 , according to a spokesman for the U.S. Marshals Service. The suspect turned herself in to the FBI November 23 at her Los Angeles attorney's office. Federal agents had been looking for her since the November 10 lockdown of the Broward County school district that caused the nearly daylong lockdowns of more than 300 schools and other government buildings. The suspect was charged with interstate communication of a threat to injure another, a violation of federal law. If convicted, she could face up to 5 years in federal prison. According to authorities, the suspect sent an e-mail from her computer to a WFTL-850 AM talk show host, and at 8:38 a.m. made a call from her cell phone to the radio station. Both messages contained threats about committing violence in government buildings, including schools, according to the FBI.
Source: http://www.orlandosentinel.com/news/local/breakingnews/fl-lockdown-woman-court-20101207,0,7333209.story

37. *December 6, Lawrence Journal-World* – (Kansas) **One person taken to LMH after emergency crews evacuate Malott Hall on KU campus; chemical smell reported in lab.** One person was taken to Lawrence Memorial Hospital (LMH) in Lawrence, Kansas and another was treated by emergency medical workers after Kansas University's (KU) Malott Hall was evacuated about 4:30 p.m. December 6 following a report of a chemical odor inside a laboratory. Crews were called to Malott Hall when the odor was detected in a fifth-floor lab, according to a university spokeswoman. Fire and hazardous materials officials reopened the building just after 6:45 p.m., when the smell had dissipated and the air quality was determined to be safe. The spokeswoman said two KU employees complained of headaches. One employee was taken to LMH, while the other was treated on the scene.
Source: http://www2.ljworld.com/news/2010/dec/06/emergency-crews-evacuate-malott-hall-ku-campus/?breaking

38. *December 6, Arkansas Democrat-Gazette* – (Arkansas) **UAMS evacuated due to discovery of acid.** The discovery of several containers of acid at the University of Arkansas for Medical Sciences (UAMS) in Fayetteville prompted a partial evacuation and response by experts in handling hazardous materials. Crews from the Fayetteville Fire Department and other agencies responded December 6 after someone discovered containers of picric acid in the facility at the corner of College Avenue and North Street. Used in controlled environments for staining microscopic samples, the chemical

under certain conditions can be explosive. Officials removed the material to vehicles equipped for hazardous materials around 11:30 a.m., and then transported it to a safe location for destruction. Workers were allowed back into the building around the same time.
Source: http://www.arkansasonline.com/news/2010/dec/06/uams-evacuated-due-discover-acid/

For another story, see item **2**

[Return to top]

Emergency Services Sector

39. *December 7, KIDK 3 Idaho Falls* – (Idaho) **Law enforcement radios turn digital.** DHS is mandating certain grant money for law enforcement to switch to digital radios. This will provide a common platform for them to all be able to talk together. "We started probably about 3 years ago, started to apply for a grant, to pay for the radio system," said an Idaho Falls Police Department captain. "The federal government wants agencies to go to what is called a P25 standard, so there is inter-operability between radios." Bonneville, Jefferson, Clark, Madison, and Fremont County in Idaho worked together to put this new radio system in place. Existing scanners will not be able to pick up the new digital radio channels, unless new digital scanners are purchased. Then they will only be able to hear the main dispatch channel, which is unencrypted. The new radios have some new features officers are excited about, like caller ID on the digital readout. "So if there is an emergency and you just push the button it comes across that I am the one that needs help. Then through GPS or whatever, it finds where the officer is at or go onto the system, if they aren't able to talk," the captain said.
Source: http://www.kidk.com/news/local/111415374.html

40. *December 7, Stockton Record* – (California) **Ex-Calaveras man arrested in Web threats against deputy.** A former Calaveras County, California resident who lives in New York has been arrested by the FBI on a firearms charge after he allegedly posted a Craigslist item asking users if they "want to ambush a Calaveras deputy." The item was posted November 22 in the Rants and Raves section of the Stockton, California-area Craigslist. A Calaveras County sheriff sergeant said a Craigslist user sent an e-mail to the sheriff's department alerting investigators to the posting. Sheriff's officials contacted Craigslist, which immediately removed the post. Investigators said they traced the posting to the 33-year-old New York man. The man used to live in Calaveras County and had been arrested there in the past. On December 2, FBI agents contacted the suspect and arrested him on a charge of being a criminal in possession of a firearm.
Source:
http://www.recordnet.com/apps/pbcs.dll/article?AID=/20101207/A_NEWS02/12070312/-1/NEWSMAP

41. *December 6, KSDK 5 St. Louis* – (Illinois) **Bomb threat at Madison County Criminal Justice Center.** A bomb threat was made against the criminal justice center in Madison County, Illinois, but the threat was ultimately deemed non-existent. According to the chief of detectives for the Madison County Sheriff's Office, the threat was made for a specific time for December 6. The investigation was launched at 2 p.m. The Madison County Criminal Justice Center was evacuated while authorities conducted their search. A bomb certified canine unit was dispatched to the building. But in the end, the building was deemed safe. A potential suspect was identified and taken into custody. The case was slated to be presented to the state attorney's office for formal charges on December 7.
Source: http://www.ksdk.com/news/local/story.aspx?storyid=231514&catid=3

[Return to top]

Information Technology Sector

42. *December 7, Help Net Security* – (International) **Search results for Mono Lake lead to malware.** The recent discovery by NASA scientists of a bacteria that uses arsenic in its cellular structure has prompted a lot of people to search the Web for information about it and the place where it was discovered — Mono Lake in California. As it had already been done with many topics that have fired up the imagination and the curiosity of a large number of people, malware peddlers have jumped to the opportunity to funnel that traffic their way and have set up an SEO poisoning campaign. Sunbelt researchers report that Google Images results have been poisoned, making certain images redirect the users to sites that try to download a rogue security tool or to fake Firefox update pages that urge them to download the supposed update for the browser. However, the offered file is a Trojan downloader.
Source: http://www.net-security.org/malware_news.php?id=1557

43. *December 7, SC Magazine UK* – (International) **2010 proves to be the year of the botnet, with new disguise and dropping capabilities expected in 2011.** Botnets remained strong in 2010 but new tactics are expected next year. According to the MessageLabs Intelligence 2010 Security Report from Symantec, spam rates peaked in August 2010 at 92.2 percent, with spam from botnets accounting for 88.2 percent of all spam. It also claimed that by the end of 2010 there was a reduction in the contribution of botnets to spam and by the end of this year to this point, the total number of active bots had returned to roughly the same number as at the end of 2009, increasing by about 6 percent in the latter half of 2010. A MessageLabs Intelligence senior analyst at Symantec Hosted Services said there are around 5 million botnets generally active at any one time, but that can vary from three and a half to five and a half million botnets. The report also found while 2010 has experienced fluctuation in the number of botnets and their associated output, the top three botnets have not changed in the latter half of 2010, with Rustock remaining the most dominant botnet, followed by Grum and Cutwail.
Source: http://www.scmagazineuk.com/2010-proves-to-be-the-year-of-the-botnet-with-new-disguise-and-dropping-capabilities-expected-in-2011/article/192300/

44. *December 6, PC Pro* – (International) **Single software license shared 774,651 times.** A single license for Avast security software has been used by 774,651 people after it went viral on a file-sharing site, according to the company. Avast noticed that a license for its paid-for security software, sold to a 14-user firm in Arizona, was being distributed online. Rather than shut down the piracy, the company decided to see how far the software would spread. The Avast Pro license showed up on file-sharing sites, and a year and a half later it had topped three-quarters of a million active users. "We found our license code at a number of warez sites around the globe," said the chief executive of Avast Software. "There is a paradox in computer users looking for 'free' antivirus programs at locations with a known reputation for spreading malware." The license is being used in 200 countries. The company is looking to flip users of the pirated version to genuine software by popping up a notice on machines with the illegally-shared edition offering a link to the free or paid-for versions.
Source: http://www.pcpro.co.uk/news/security/363379/single-software-licence-shared-774-651-times

45. *December 6, Softpedia* – (International) **Binary planting vulnerability fixed in Adobe Illustrator CS5.** A security and stability update has been released for Adobe Illustrator CS5, fixing a DLL preloading vulnerability which could be exploited to execute arbitrary code. Since files can be loaded directly from network shares or WebDAV resources, this arbitrary code execution condition also has a remote attack vector. The vulnerability in Adobe Illustrator CS5 is identified as CVE-2010-3152 and Adobe rates it as "important." Users of Illustrator CS 15.0.1 or earlier are strongly advised to install the 15.0.2 update as soon as possible. In addition to the security content, this update contains a series of other bug fixes.
Source: http://news.softpedia.com/news/Binary-Planting-Vulnerability-Fixed-in-Adobe-Illustrator-CS5-170878.shtml

46. *December 6, TechWorld* – (International) **Internet Explorer 'protected mode' weakness spelled out.** Researchers have found a chink in Internet Explorer's "protected mode" security armor that hints at trouble for other Windows apps built around the technology, including Google's Chrome and Adobe's new Reader X. In a new paper, Verizon Business researchers document ways that an attacker could elevate the privileges of a process to zones where Protected Mode would not apply, such as the local intranet network (which uses UNC paths) or by spoofing the trusted sites list. This leads to the possibility of a relatively simple attack in which malware executes as a low priority process which creates a virtual Web server tied to a local software "loopback" port. Although this process will also be shut out by protected mode, it would be able to point IE to a Web address which appears to be in the Local Internet Zone. By this point, the Web page will be able to render at medium integrity, a potentially dangerous privilege escalation. The weakness found by Verizon does not directly affect other applications that use protected mode security, such as Adobe Reader X or Google Chrome, but it does show how such protection mechanisms will remain open to attack based on the fact that some elements of a system have to be trusted.
Source: http://www.networkworld.com/news/2010/120610-internet-explorer-protected-mode-weakness.html

47. *December 3, The Register* – (International) **Popular sites caught sniffing user browser history.** Security experts from Southern California have caught YouPorn.com and 45 other sites pilfering visitors' surfing habits in what is believed to be the first study to measure in-the-wild exploits of a decade-old browser vulnerability. YouPorn uses JavaScript to detect whether visitors have recently browsed to PornHub.com, tube8.com and 21 other sites, according to the study. It tracked the 50,000 most popular Web sites and found a total of 46 other offenders, including news sites charter.net and newsmax.com, finance site morningstar.com, and sports site espnf1.com. "We found that several popular sites — including an Alexa global top-100 site — make use of history sniffing to exfiltrate information about users' browsing history, and, in some cases, do so in an obfuscated manner to avoid easy detection," the report states. "While researchers have known about the possibility of such attacks, hitherto it was not known how prevalent they are in real, popular websites." The 46 sites exploit a widely known vulnerability that currently exists in all production version browsers except of Apple's Safari. The study also detected code on sites maintained by Microsoft, YouTube, Yahoo, and About.com that perform what the scientists called "behavioral sniffing." Source: http://www.theregister.co.uk/2010/12/03/browser_history_sniffing/

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

48. *December 7, The Register* – (International) **Hacker brings enhanced security to jailbroken iPhones.** A computer consultant is adding a security measure known as ASLR to iPhones to make them more resistant to malware attacks. Short for address space layout randomization, ASLR has been absent from all iOS devices since their inception, making possible the types of attacks that commandeered a fully patched iPhone at the Pwn2Own hacker contest. By randomizing the memory locations where injected code is executed, ASLR aims to thwart such exploits by making it impossible to know ahead of time where malicious payloads are located. Starting with Windows Vista, Microsoft has baked ASLR into its operating system, and the recently released mobile version of Windows 7 is also endowed with the protection, said the principal security analyst at Independent Security Evaluators, who cited private conversations with Microsoft engineers. By comparison, Apple has built only limited ASLR into Mac OS X and has left it out of iOS altogether. At a conference scheduled for the week of December 13, a security consultant and application developer for Germany-based SektionEins, plans to unveil a process for jailbreaking iDevices that automatically fortifies them with ASLR. It works by reordering the contents of dyld_shared_cache, a

massive file that houses the libraries.
Source: http://www.theregister.co.uk/2010/12/07/enhanced_iphone_security/

49. *December 6, eWeek* – (National) **DNSSEC Adoption Jumps, But Users Fail to Maintain It Properly: Survey.** More and more organizations are implementing DNSSEC on their name servers. But the actual number of signed zones is very low, leaving these organizations vulnerable to cache poisoning attacks. While organizations are beginning to adopt DNSSEC (Domain Name System Security Extensions) to secure their Web sites, most of them have not correctly implemented or maintained according to specifications, according to a survey released by Infoblox December 6. The sixth annual survey of domain name server infrastructure on the Internet is a "census of name servers," the vice-president of architecture at Infoblox said. The survey identified 15.6 million name servers on the Internet and included only the .org, .com and .net domains, he said. While adoption of the DNS Security Extensions jumped a dramatic 340 percent from 2009, the actual number of "zones" that have been signed is less than 1 percent, the survey said. Considering that organizations went through the trouble of setting up the DNSSEC on their name servers, the fact that only 0.022 percent of the zones were signed was "surprisingly high" and a "clear indicator" they weren't configuring or maintaining them correctly, the vice president said. In 2009, the number was even smaller, at 0.005 percent, he said. DNSSEC is a set of security extensions that authenticate DNS data to ensure the Web servers the public connects to are authentic and not run by malicious imposters. In a cache poisoning attack, a cybercriminal directs users to a different Web site without their realizing it.
Source: http://www.eweek.com/c/a/Security/DNSSEC-Adoption-Jumps-But-Users-Fail-to-Maintain-It-Properly-Survey-261017/

[Return to top]

Commercial Facilities Sector

50. *December 6, Knoxville News Sentinel* – (Tennessee) **Two-alarm fire guts Mt. Calvary.** A massive fire gutted the sanctuary of Mt. Calvary Baptist Church in East Knoxville, Tennessee, December 5. No injuries were reported in what Knoxville firefighters called one of the larger structural fires they had seen since the historic McClung warehouses caught fire downtown in February 2007. The Knoxville Fire Department (KFD) responded at 4:42 p.m. to the initial report of heavy smoke in the church at 1807 Dandridge Ave. Eight parishioners inside smelled smoke and walked toward the older side of the church to investigate. The church members escaped unharmed. Some 30 KFD firefighters from five surrounding stations responded, shutting down Dandridge Avenue with more than a half-dozen fire trucks. Reserve engines and off-duty personnel were expected to be called in to maintain a steady stream of water on the building and monitor it for flare-ups throughout the night. Fire investigators also were expected to return to the scene to determine the fire's cause.
Source: http://www.knoxnews.com/news/2010/dec/06/two-alarm-fire-guts-mt-cavalry/

51. *December 6, Dallas Morning News* – (Texas) **Bomb threat called into Dallas Country Club on Sunday.** A caller who said a former U.S. President owed him $50 million is thought to be responsible for the threats that forced police to close the Dallas Country Club in Dallas, Texas December 5. The man, who also identified himself as a former employee of the club, is also linked to similar threats made against country clubs in Austin, Midland, and San Antonio, according to police reports provided by a Highland Park police officer. A police report indicates he is known to the U.S. Secret Service as an "unverified threat" and a mentally disturbed person. Highland Park officers closed the club December 5 and contacted federal authorities, as well as other Texas cities where similar threats were made. Employees searched the club and found nothing suspicious.
Source: http://parkcitiesblog.dallasnews.com/archives/2010/12/bomb-threat-called-into-dallas.html

52. *December 6, KFDM 6 Beaumont* – (Texas) **Beaumont hotel evacuated after fire.** A small fire forced the evacuation of one of the largest hotels in Beaumont, Texas, December 6. Firefighters received a call around 6:05 p.m. about smoke being reported at the MCM Elegante on Interstate 10 near Washington. Smoke was reported on several floors. The hotel guests were safely evacuated as firefighters went floor by floor, looking for the cause of the smoke. After several hours of investigating, they found a small fire in the duct work on the 9th floor. The guests staying on that floor had to be relocated to other rooms in the hotel for the night. The cause of the fire is under investigation.
Source: http://www.kfdm.com/news/fire-40525-floor-hotel.html

53. *December 6, WJXT 4 Jacksonville* – (Florida) **Ammo explosions in store could be heard.** Explosions of live rounds of ammunition and lighter fluid inside a military surplus store that caught fire December 5 drew a massive response by Jacksonville Fire Rescue in Jacksonville, Florida. Firefighters lined Roosevelt Boulevard for about a half mile from Patriot Mania on Yukon Road at about 1 a.m. The flames were not spreading beyond the building, but ammo inside that was exploding was the main cause for concern, firefighters said. They said the rounds could be heard going off inside the store when they arrived. It took about half an hour to extinguish the fire, which, according to store surveillance, started from beneath a display case. Investigators do not suspect arson. No one was hurt in the fire.
Source: http://www.news4jax.com/news/26036326/detail.html

54. *December 6, KRTV 3 Great Falls* – (Montana) **Grenade triggers evacuation at Easter Seals-Goodwill.** A suspicious package delivered to Easter Seals-Goodwill in Great Falls, Montana, triggered the evacuation of nearly 100 people December 6. Just before 10 a.m., an item that looked like a grenade was found among the donations at the facility, located at 4400 Central Avenue. Great Falls police and the Explosive Ordnance Disposal team from Malmstrom Air Force Base were called in to investigate. The donated item was, in fact, a grenade, but it had been hollowed out. The grenade was taken by the Malmstrom EOD unit for disposal. Everyone was allowed back into the building by 11:30 a.m.

Source: http://www.krtv.com/news/grenade-triggers-evacuation-at-easter-seals-goodwill/

55. *December 5, WFAA 8 Dallas-Fort Worth* – (Texas) **Guest killed in Fort Worth motel fire.** A man died December 5 when a fire broke out in his Fort Worth, Texas motel room. A Fort Worth Fire Department spokesman said the first alarm went out at 4:12 a.m. at the Century Motel, 3434 East Lancaster Avenue. Firefighters found the victim "in heavy fire conditions" in Room 209. He was pronounced dead at the scene. No identity was released. A charred oxygen tank was among the debris. A tenant told News 8 that the victim had been smoking in his room, but there was no official confirmation of that account. Seventeen people who live in the 65-year-old building were displaced by the fire and a resulting electrical outage. The cause of the fire was under investigation.
Source: http://www.wfaa.com/news/local/Guest-killed-in-Fort-Worth-motel-fire-111348694.html

[Return to top]

National Monuments and Icons Sector

56. *December 6, Associated Press* – (California) **Leaking mine near Patagonia to be sealed.** A contractor for the U.S. Forest Service will seal an old mine near Patagonia, California, that has been leaking highly acid water for decades. The main contractor will install two watertight plugs in the horizontal tunnel leading into the World's Fair Mine on the Coronado National Forest. The work is expected to be complete by late spring, 2011. The plugs are designed to keep water from entering the mine and acidized water from running out of the mine.
Source: http://www.businessweek.com/ap/financialnews/D9JUGOE80.htm

57. *December 6, New York Times* – (National) **In the wild, a big threat to rangers: humans.** The dangers to park rangers were highlighted in November 2010, when a Pennsylvania wildlife officer was killed by an illegal hunter. The two recent shootings of wildlife officers — the one killed in Pennsylvania while confronting an illegal hunter, the other seriously wounded after a traffic stop in southern Utah — have highlighted what rangers and wildlife managers said is an increasingly unavoidable fact. As more and more people live close to forests, parks and other wild-land playgrounds, the human animal, not the wild variety, is the one to watch out for. Guns became legal in many National Parks this year under a law enacted by Congress in 2009. Many parks and recreation areas around the nation have also suffered staff cuts in recent years, reducing the presence of badge-wearing authority figures on patrol. Fifteen wildlife or park employees have been killed on duty, most of them by gunshot, since 1980, according to the North American Wildlife Enforcement Officers Association.
Source: http://www.nytimes.com/2010/12/07/us/07rangers.html

[Return to top]

Dams Sector

58. *December 6, WDSU 6 New Orleans* – (Louisiana) **Corps wants to raise Westbank Levee.** The U.S. Army Corps of Engineers wants to raise a 15-mile stretch of levee from English Turn in New Orleans, Louisiana to Oakville south of Belle Chasse. Some temporary work on the levee is already under way. The Corps said the westbank levee was designed to protect against high river water, not hurricane-strength storm surge. If the Corps approves the project, it could be completed by next summer.
Source: http://www.wdsu.com/news/26039365/detail.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/iaipdailyreport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer